Київський національний торговельно-економічний університет

Кафедра менеджменту

ВИПУСКНА КВАЛІФІКАЦІЙНА РОБОТА

на тему:

«Формування інформаційної безпеки підприємства»

(за матеріалами АТ **«**Банк ¾**»**, м. Київ)

Студентки 3 курсу 10с групи
спеціальності 073 «Менеджмент»
спеціалізації «Управління
бізнесом» _____ Беднякової Лоліти Олегівни

Науковий керівник:
кандидат економічних наук,
доцент _____ Хмурова Вікторія Валентинівна

Гарант освітньої програми:
кандидат економічних наук,
доцент _____ Підкамінний Ігор Миколайович

Київ 2022

Київський національний торговельно-економічний університет

Факультет_____економіки, менеджменту та психології_____
Кафедра _____*менеджменту*_____
Освітній ступінь_____*бакалавр*_____
Спеціальність _____*073 Менеджмен*т_____
Спеціалізація _____*Управління бізнесом*_____

Затверджую

Зав. кафедри
Бай Сергій Іванович
«____» _____2021 р.

Завдання
на випускну кваліфікаційну роботу студенту

_____Бедняковій Лоліті Олегівні_____
(прізвище, ім'я, по батькові)

1. Тема випускної кваліфікаційної роботи
Формування інформаційної безпеки підприємства
_____
_____

Затверджена наказом ректора від «_02_» _грудня__2021_____ №__4009___

2. Строк здачі студентом закінченої роботи _____
3. Цільова установка та вихідні дані до роботи

Мета роботи _____розробка управлінських рішень, щодо покращення інформаційної безпеки підприємства.
_____
_____

Об'єкт дослідження _____інформаційна безпека підприємства в цілому_____
_____

Предмет дослідження _____теоретичні та методологічні основи інформаційної безпеки в середині компанії_____
_____

4. Консультанти по роботі із зазначенням розділів, за якими здійснюється консультування:

Розділ	Консультант (прізвище, ініціали)	Підпис, дата	
		Завдання видано	Завдання виконано

5. Зміст випускної кваліфікаційної роботи (перелік питань за кожним розділом)

РОЗДІЛ 1 КОНЦЕПТУАЛЬНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

РОЗДІЛ 2 АНАЛІЗ ГОСПОДАРСЬКОЇ ДІЯЛЬНОСТІ БАНКУ “БАНК ¾”

2.1 Аналіз фінансово-економічної діяльності банку

2.2 Аналіз інформаційної безпеки банку

РОЗДІЛ 3 РОЗРОБКА ЗАХОДІВ ПОКРАЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ

3.1 Розробка заходів покращення інформаційної безпеки

3.2 Оцінка ефективності запропонованих рішень

_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____
_____

6. Календарний план виконання випускної кваліфікаційної роботи

№ з/п	Назва етапів випускної кваліфікаційної роботи	Строк виконання етапів роботи	
		за планом	фактично
1	*2*	*3*	*4*
1.	Визначення напряму дослідження та затвердження теми випускної кваліфікаційної роботи	до 19.11.21 р.	
2.	Складання плану та підготовка індивідуального завдання для виконання випускної кваліфікаційної роботи	до 06.12.21 р.	
3.	Рецензування планів випускної кваліфікаційної роботи	до 17.12.21 р.	
4.	Направлення студентів на об'єкти виробничої практики	згідно графіка навч. процесу	
5.	Збір статистичних даних, підготовка аналітичного матеріалу випускної кваліфікаційної роботи	до 17.01.21 р.	
6.	Періодичне звітування студентів про виконання випускної кваліфікаційної роботи перед науковими керівниками та завідувачем кафедри	з 10 по 20 число щомісяця	
7.	Представлення закінченої випускної кваліфікаційної роботи на кафедру (з листом-відгуком з підприємства) та її реєстрація	до 20.01.22 р.	
8.	Підготовка відгуку на випускну кваліфікаційну роботу науковим керівником	до 24.01.22 р.	
9.	Проведення попереднього захисту випускної кваліфікаційної роботи	24.01.22 р. - 25.01.22 р.	
10.	Вирішення питання про допуск випускної кваліфікаційної роботи до захисту	Згідно графіка	
11.	Проходження зовнішнього рецензування	Згідно графіка	
12.	Направлення випускної кваліфікаційної роботи із зовнішньою рецензією у ЕК для захисту	Згідно графіка	
13.	Захист випускної кваліфікаційної роботи в комісії	Згідно графіка навч. процесу	

7. Дата видачі завдання «_03_»__грудня____2021 р.

8. Науковий керівник випускної кваліфікаційної роботи
_____Хмурова В.В._____
(прізвище, ініціали, підпис)

9. Гарант освітньої програми _____Підкамінний І.М._____
(прізвище, ініціали, підпис)

10. Завдання прийняв до виконання студент _____Беднякова Л.О._____
(прізвище, ініціали, підпис)

11. Відгук наукового керівника випускної кваліфікаційної роботи

____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____
____

Науковий керівник випускної кваліфікаційної роботи ______________________

(підпис, дата)

Відмітка про попередній захист ____

(ПІБ, підпис, дата)

12. Висновок про випускну кваліфікаційну роботу

Випускна кваліфікаційна робота студента ________________________________

(прізвище, ініціали)

може бути допущена до захисту екзаменаційній комісії.

Гарант освітньої програми ____

(прізвище, ініціали, підпис)

Завідувач кафедри ____

(підпис, прізвище, ініціали)

«_____» ___________________20___ р.

ДТЕУ ДЕРЖАВНИЙ ТОРГОВЕЛЬНО-ЕКОНОМІЧНИЙ УНІВЕРСИТЕТ

РЕФЕРАТ

випускної кваліфікаційної роботи бакалавра,
виконаної на тему: **«Формування інформаційної безпеки підприємства»**

Структура роботи. Випускна кваліфікаційна робота бакалавра викладена на 36 сторінках основного тексту, в т.ч. містить 5 таблиць та 4 рисунки. Список використаних джерел містить 19 найменувань, викладених на 2-х сторінках. Робота містить 3 додатки, викладен на 7 сторінках.

Метою дослідження є розробка управлінських рішень, щодо покращення інформаційної безпеки підприємства.

Відповідно до поставленої мети, сформульовано перелік *завдань* для виконання в процесі даного наукового дослідження:

- досліджено концептуальні засади інформаційної безпеки;
- проаналізовано фінансово-економічну діяльність підприємства;
- проаналізувано інформаційну безпеку підприємства;
- розроблено заходи для покращення інформаційної безпеки на підприємстві;
- оцінено ефективність запропонованих рішень.

Об'єктом дослідження є інформаційна безпека підприємства в цілому. *Предметом дослідження* є теоретичні та методологічні основи інформаційної безпеки в середині компанії.

Одержані результати можуть бути використані та впровадженні у АТ "Банк ¾"

Рік виконання роботи 2021- 2022 рр.

Рік захисту роботи – 2022 р.

Анотація

кваліфікаційної роботи, виконаної на тему:

«Формування інформаційної безпеки підприємства»

(за матеріалами АТ "Банк ¾", м. Київ)

Випускна кваліфікаційна робота бакалавра присвячена дослідженню формування інформаційної безпеки у банківській установі. У роботі вирішено важливе науково-практичне завдання, щодо подальшого розвитку теоретичних основ, методичних і практичних пропозицій та рекомендацій з удосконалення інформаційної безпеки банку.

Досліджено динаміку основних показників діяльності підприємства протягом 2018-2021 років з метою розробки програми покращення інформаційної безпеки на підприємстві, оцінено ефективність запровадження нового програмного забезпечення на підприємстві.

Ключові слова: інформаційна безпека, банківська установа, банківська таємниця, методи передачі інформації, готовність підприємства до змін, ефективність проведення змін.

Annotation

final qualifying paper performed on the theme:

«Formation of information security of the enterprise»

(based on materials JSC «Bank 3/4», Kyiv)

Final qualification paper of the bachelor is devoted to the study of the formation of information security in a banking institution. The paper solves an important scientific and practical task of further development of theoretical foundations, methodological and practical proposals and recommendations for improving information security of the bank.

The dynamics of the main indicators of the enterprise during 2018-2021 is studied in order to develop a program to improve information security at the enterprise, the effectiveness of the introduction of new software at the enterprise is assessed.

Keywords: information security, banking institution, banking secrecy, methods of information transfer, enterprise readiness for change, efficiency of changes.

ЗМІСТ

ВСТУП

У сучасному світі все більше уваги приділяється захисту інформації. Як і в будь-якому іншому виді діяльності, грамотне планування забезпечення безпеки інформації є найважливішим етапом на шляху до забезпечення безпеки даних.

Зміни, що відбулись в останні роки у суспільному житті, політиці, економіці, науковій сфері призвели до значного зростання обсягів інформації. За таких умов сформувалась ситуація за якої виник ризик використання даних про підприємство проти нього самого. А отже виникла неабияка потреба у забезпеченні захисту, а точніше інформаційної безпеки.

Організація ефективної системи захисту інформації стає критично важливим стратегічним чинником розвитку та напряму впливає на темпи зростання, позицію на ринку та рівень довіри клієнтів та партнерів до компанії. Так або інакше, сьогодні всі великі і процвітаючі комерційні структури розвинених держав мають в своєму штаті підрозділи, які займаються інформаційною діяльністю. У одних фірмах - це інформаційно-аналітичний відділ, в інших - відділ маркетингу, на який керівництво фірми разом з іншими покладає і інформаційно-аналітичні завдання, в третіх - відділ комерційної розвідки. Часто все залежить від рівня розуміння керівництвом фірми ступеня важливості інформаційно-аналітичної роботи для безпеки всіх сторін діяльності будь-якої комерційної структури.

Особливість безпеки інформаційної діяльності полягає у запобіганні, протидії та подоланні природних (стихійних), техногенних і соціогенних (антропогенних) загроз, здатних порушити (чи припинити) життєдіяльність конкретного суб'єкта (людини, соціальних спільнот, суспільства, держави, світового співтовариства), у тому числі підприємництва, чим і визначається актуальність теми дослідження.

Метою випускної кваліфікаційної роботи є розробка управлінських рішень, щодо покращення інформаційної безпеки підприємства.

Основними завданнями, які повинні допомогти досягти поставленої мети, є:

- дослідити концептуальні засади інформаційної безпеки;
- проаналізувати фінансово-економічну діяльність підприємства;
- проаналізувати інформаційну безпеку підприємства;
- розробити заходи для покращення інформаційної безпеки на підприємстві;
- оцінити ефективність запропонованих рішень.

Об'єкт дослідження - інформаційна безпека підприємства в цілому.

Предмет – теоретичні та методологічні основи інформаційної безпеки в середині компанії.

Для написання випускної кваліфікаційної роботи було використано літературу по темі, актуальні Закони України та інтернет ресурси.

Дана випускна кваліфікаційна робота має практичне значення для підприємства, оскільки впровадження нових методів роботи з інформацією, покращує загальний рівень продуктивності банку та підвищує рівень інформаційної безпеки. В підтвердження наведено лист-відгук з підприємства.

Основний текст роботи (до початку списку використаних джерел) становить 34 сторінки, в т.ч. 5 таблиць, 4 рисунки. Список використаних джерел містить 19 найменувань, викладених на 2 сторінках. Випускна кваліфікаційна робота містить 3 додатки, викладені на 7 сторінках.

РОЗДІЛ 1 КОНЦЕПТУАЛЬНІ ЗАСАДИ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ

Враховуючи, що інформаційні проблеми, які постали перед суспільством в останні роки стали досить актуальними, їм було присвячено значну кількість досліджень, у різних сферах діяльності. Беручи до уваги підприємницьку діяльність можна звернути увагу на роботи Когута Ю.І., Марущака А.І., Кормича Б.А., Берлача А.І., Ніколаюка С.І., Никифорчука Д.Й., Позднишева Є.В., Вертузаєва М.С. (Україна), К. Богана, М. Інгліш, Д. Прескота, С. Міллера (Великобританія). Корисними можуть бути матеріали викладені в роботах вітчизняних науковців Панченко О.А. та Банчука М.В., Єщенко П.С. та Арсеєнко А.Г., Прибутько П.С. та Лук'янця І.Б., Остроухова В.В. Роботи зазначених авторів є цікаві не лише своїм змістом, головне це точки зору, міркування, позиції авторів, які вони обґрунтовують і які дають підґрунтя для творчого розуміння проблем, що виникли в інформаційному просторі вітчизняного підприємництва та вироблення підходів до їх подолання, побудови адекватних систем інформаційної безпеки.

Інформаційна безпека - це стан захищеності систем обробки і зберігання даних, при якому забезпечено конфіденційність, доступність і цілісність інформації використання й розвиток в інтересах громадян або комплекс заходів, спрямованих на забезпечення захищеності інформації особи, суспільства і держави від несанкціонованого доступу, використання, оприлюднення, руйнування, внесення змін, ознайомлення, перевірки запису чи знищення [8].

Кажучи про безпеку інформації не можна не згадати інформаційні технології, які якраз, і потребують захисту, або сприяють йому (рис.1.1). Звідси, опанування такими технологіями виступає обов'язковою умовою життєдіяльності та розвитку підприємства. Особливо це характерно для ринкових умов, де діяльність суб'єктів підприємництва здійснюється під

впливом конкуренції. А конкурентні переваги якраз і базуються на сучасних та перспективних технологіях.

Рис.1.1 Інформаційні технології

Оскільки підприємство знаходиться у постійному русі, то необхідно підлаштовувати методи роботи з інформацією, в залежності від змін, що стаються. А саме:

- бути у постійному пошуку необхідної інформації і формування власного інформаційного ресурсу;
- враховувати неоднозначну структуру та якость інформації, що перебуває в інформаційному середовищі, бути готовими до її постійного аналізу;
- використовувати сучасні інформаційні технології та досягнення інформаційного розвитку у виробничому процесі;
- бути здатними ефективно захищати свій інформаційний ресурс, бути готовими до протидії інформаційному впливу та підтриманню на необхідному рівні свого іміджу;
- забезпечувати інформаційний вплив на ринок з метою формування позитивних перспектив свого розвитку;
- оволодіти методами здійснення інформаційного протиборства та інформаційної війни, забезпечувати виживання в умовах їх

проведення;

- зберігати інформаційну інфраструктуру в умовах проведення актів кібертероризму.

Ще одне важливе явище, яке витікає з вищесказаного - інформаційні відносини. З практики застосування термінів, слів та словосполучень у юриспруденції під інформаційними відносинами розуміють суспільні відносини, що виникають у всіх сферах життя і діяльності суспільства й держави при одержанні, використанні, поширенні і зберіганні інформації. Або, якщо більш коротко: інформаційні відносини — суспільні відносини, які виникають при збиранні, одержанні, зберіганні, використанні, поширенні та захисту (охороні) інформації.

Можна говорити, що інформаційні відносини виникають там де їх предметом є будь-які дії з інформацією. Причому, не має значення вид інформації чи її стан (електронна, документована інформація, знання і т. д.). Відповідно до зазначеного закону основними принципами інформаційних відносин мають бути: гарантованість права на інформацію, відкритість, доступність інформації, свобода обміну інформацією, достовірність і повнота інформації, свобода вираження поглядів і переконань, правомірність одержання, використання, поширення, зберігання та захисту інформації, захищеність особи від втручання в її особисте сімейне життя. Суб'єктами інформаційних відносин є: фізичні та юридичні особи, об'єднання громадян, суб'єкти владних повноважень. Об'єктом інформаційних відносин є інформація.

Враховуючи зміст поняття «інформаційних відносин» та їх суб'єктно-об'єктну сторону, можна говорити про об'єктивність виникнення таких відносин і поміж суб'єктами, що здійснюють підприємницьку діяльність. Тут слід звернути увагу на те, що інформаційні відносини виникають не лише у зв'язку з інформаційною діяльністю як видом підприємництва, вони можуть виникати у будь-якій сфері діяльності. Згідно чинного законодавства, право на інформацію (вільне одержання, використання, поширення, зберігання,

захист інформації, необхідної для реалізації законних інтересів) не обмежується видом діяльності в т. ч. і у сфері підприємництва. В той же час, реалізація права на інформацію не повинна порушувати громадські, політичні, економічні, соціальні, духовні, екологічні та інші права, свободи і законні інтереси інших громадян, права та інтереси юридичних осіб. Стосовно підприємницької діяльності важливим є неприпустимість порушення економічних та інших прав і інтересів суб'єктів підприємництва у процесі одержання, використання, поширення, зберігання, захисту інформації.

Такі особливості реалізації права на інформацію є важливими у випадках регулювання доступу до інформації суб'єктів підприємництва, яка має обмежений доступ, їх захисту при поширенні інформації, що шкодить їх діловій репутації, обмежує діяльність на ринку, а також протидії використанню інформаційних технологій для викривлення інформаційних характеристик суб'єктів в конкурентній боротьбі.

Говорячи про економічні права необхідно зазначити, що такі права передбачають: право здійснення будь-якої суспільної діяльності не забороненої законом, в т. ч. і в підприємництві, право вільно обирати вид і місце діяльності, її обсяги, бути незалежним у такій діяльності, право на захист своєї діяльності і власності, право вільного розпорядження результатами діяльності, інші права.

Як показує практика підприємницької діяльності реалізація зазначених прав здійснюється в т. ч. і через інформаційну сферу. Крім суто економічного змісту діяльності остання наповнена великою кількістю інформаційних характеристик. Тому вступаючи у економічні (виробничі, фінансові, комерційні) відносини суб'єкти підприємництва обов'язково торкаються таких характеристик. Більш того, інколи зазначені характеристики відіграють провідну роль у взаємовідносинах, оскільки розкривають економічний зміст, природу, напрямки розвитку діяльності суб'єктів та їх взаємовідносин. Тому економічні взаємовідносини, в які вступають суб'єкти підприємництва

одночасно передбачають і взаємовідносини інформаційного характеру. Зазвичай у таких взаємовідносинах мають місце:

- передача інформації від одного суб'єкта до іншого, оскільки взаємовідносини неможливі без взаємоінформування суб'єктами один одного про певні аспекти своєї діяльності;
- зберігання та захист інформації: у процесі взаємовідносин суб'єкти забезпечують захист своїх технологій, знань, інтелектуальних надбань;
- поширення інформації: з метою впливу на ринок суб'єкти розробляють рекламні, іміджеві заходи та технології подачі їх в інформаційний простір;
- використання інформації, що передбачає встановлення правил користування інформаційними продуктами, загалом інформацією. Основним тут виступає принцип «не зашкодити», тобто інформація яка використовується суб'єктами не повинна шкодити їх репутації і діяльності.

Підтримуючи взаємовідносини суб'єкти підприємництва стосовно інформації можуть виступати її джерелами, споживачами (користувачами), власниками (авторами). Основними умовами інформаційних взаємовідносин можуть виступати: умови доступу до інформації, умови конфіденційності, вимоги до об'єктивності інформації, умови її використання та поширення, умови відповідальності, контроль інформації та дій щодо неї.

Таким чином, інформація є одним із головних атрибутів діяльності не лише самих суб'єктів підприємництва, а і взаємовідносини поміж ними.

Разом з тим, така роль інформації обумовлює досить високу уразливість суб'єктів підприємництва. Останні, як суб'єкти інформаційних відносин, можуть зазнавати шкоди суто через порушення таких відносин: неправомірне використання чи поширення критичної (небезпечної) для них інформації; незкоординоване або неузгоджене використання технологій інформаційного впливу, або ж їх використання на шкоду одній із сторін. Причому шкода може наступати як матеріального, так і морального

(іміджевого) характеру. Більш того, подібні порушення в інформаційних взаємовідносинах згодом можуть призводити до їх руйнування, конкуренції, в т. ч. і недобросовісної, а то і протиборства в інформаційному просторі. Така ситуація є досить небезпечною для суб'єктів підприємництва принаймні двома факторами:

- Функціонування інформації зачіпає значні маси суспільства і будь-які події у взаємовідносинах бізнес-партнерів, конкурентів чи взагалі підприємців можуть швидко ставати відомими широкому загалу. Механізми функціонування суб'єктів підприємництва в інформаційному просторі зачіпають саме головне для бізнесу – зв'язки, як у економічній, так і в політичній, владній сферах.
- Враховуючи, що інформаційні відносини носять масовий характер всі події, які в них відбуваються обов'язково когось зачіпають, для когось стають цікавими, а для когось є предметом широкої дискусії та оцінки.

Фактори, умови, явища і події під впливом яких порушується інформаційна безпека, вважаються загрозами.

Класифікацію загроз інформаційної безпеки показано на рис.1.2.

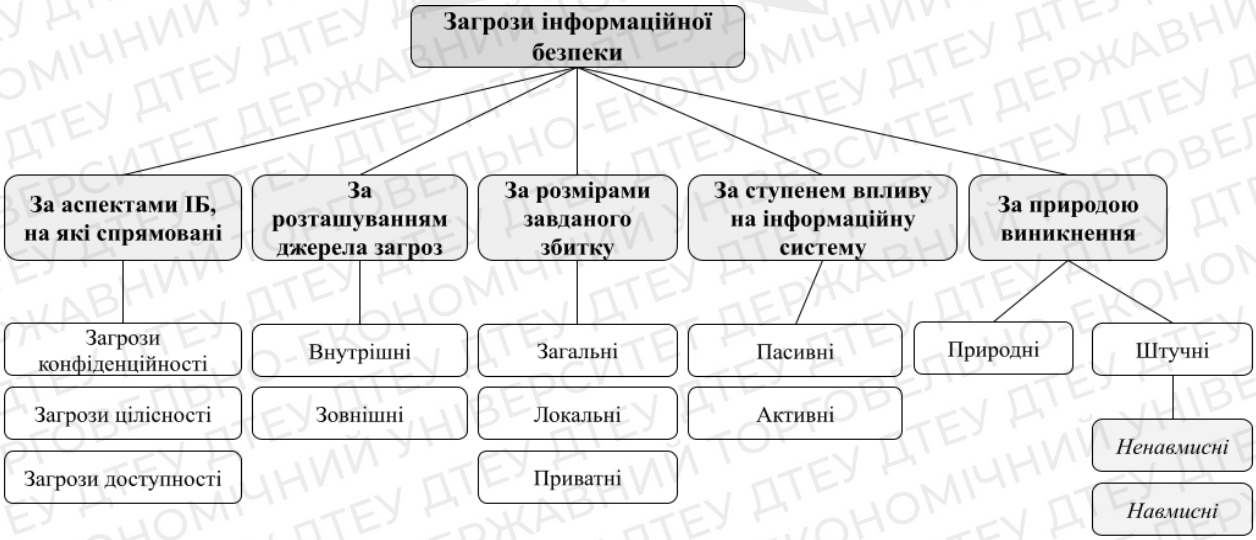

Рис. 1.2 Класифікація загроз інформаційної безпеки

Розберемо дану класифікацію більш детально:

- Загрози конфіденційності або неправомірний доступ до інформації полягає в тому, що інформація стає відомою тому, хто не володіє повноваженнями доступу до неї. Вона має місце, коли отримано доступ до деякої інформації обмеженого доступу, що зберігається в комп'ютерній системі або передається від однієї системи до іншої. У зв'язку з загрозою порушення конфіденційності, використовується термін «витік». Подібні загрози можуть виникати внаслідок «людського фактора» (наприклад, випадкове делегування тому або іншому користувачеві привілеїв іншого користувача), збоїв роботи програмних та апаратних засобів. До інформації обмеженого доступу належить державна таємниця (комерційна таємниця, персональні дані, професійні види таємниці: лікарська, адвокатська, банківська, службова, нотаріальна таємниця страхування, слідства й судочинства, листування, телефонних переговорів, поштових відправлень, телеграфних або інших повідомлень (таємниця), відомості про сутність винаходу, корисної моделі або промислового зразка до офіційної публікації (ноу-хау) та ін).
- Загрози цілісності (неправомірна зміна даних). Загрози порушення цілісності — це загрози, пов'язані з імовірністю модифікації тієї чи іншої інформації, що зберігається в інформаційній системі. Порушення цілісності може бути викликано різними чинниками — від умисних дій персоналу до виходу з ладу обладнання.
- Загрози доступності (здійснення дій, які унеможливлюють чи ускладнюють доступ до ресурсів інформаційної системи). Порушення доступності являє собою створення таких умов, при яких доступ до послуги або інформації або заблокований, або можливий за час, який не забезпечить виконання тих чи інших бізнес-цілей.
- Внутрішні (джерела загроз розташовуються всередині системи).
- Зовнішні (джерела загроз знаходяться поза системою).

- Загальні (завдавання збитку об'єкту безпеки в цілому, заподіяння значної шкоди).
- Локальні (заподіяння шкоди окремими частинами об'єкта безпеки).
- Приватні (заподіяння шкоди окремим властивостям елементів об'єкта безпеки).
- Пасивні (структура і зміст системи не змінюються).
- Активні (структура і зміст системи піддається змінам).
- Природні (об'єктивні) — викликані впливом на інформаційне середовище об'єктивних фізичних процесів або стихійних природних явищ, що не залежать від волі людини.
- Штучні (суб'єктивні) — викликані впливом на інформаційну сферу людини. Серед штучних загроз у свою чергу виділяють:
    - Ненавмисні (випадкові) погрози, помилки програмного забезпечення, персоналу, збої в роботі систем, відмови обчислювальної та комунікаційної техніки.
    - Навмисні (умисні) загрози — неправомірний доступ до інформації, розробка спеціального програмного забезпечення, використовуваного для здійснення неправомірного доступу, розробка та поширення вірусних програм і т. д. Навмисні загрози зумовлені діями людей. Основні проблеми інформаційної безпеки пов'язані насамперед з умисними погрозами, оскільки вони є головною причиною злочинів і правопорушень.

РОЗДІЛ 2 АНАЛІЗ ГОСПОДАРСЬКОЇ ДІЯЛЬНОСТІ БАНКУ “БАНК ¾”

2.1 Аналіз фінансово-економічної діяльності банку

Ліквідність характеризує здатність підприємства швидко перетворити активи на гроші. Оцінюючи ліквідність підприємства, аналізують достатність поточних (оборотних) активів для погашення поточних зобов’язань – короткострокової кредиторської заборгованості.

Ліквідність підприємства в короткостроковому періоді визначається його можливостями покрити свої короткострокові зобов’язання. Під короткостроковим періодом умовно розуміють строк до одного року, хоча іноді він також ототожнюється з операційним циклом.

Існує кілька ступенів ліквідності. Недостатня ліквідність, як правило, означає, що підприємство не може скористатися вигідними комерційними можливостями, що виникають. На цьому рівні недостатня ліквідність означає, що немає свободи вибору, і це обмежує свободу дій керівництва.
Більш значна нестача ліквідності свідчить про те, що підприємство не може оплатити свої поточні борги та зобов’язання. Це може призвести до інтенсивного продажу довгострокових вкладень та активів, а в найгіршому випадку – до неплатоспроможності та банкрутства.

Для власників підприємства недостатня ліквідність може означати зменшення прибутковості, втрату контролю та часткову або повну втрату вкладень капіталу. У випадку, коли власники несуть необмежену відповідальність, їх збитки можуть навіть перевищити початкові вкладення.

Ось чому ліквідності надається таке важливе значення. Якщо підприємство не може погасити свої поточні зобов’язання по мірі того, як настає строк їх оплати, його подальше існування ставиться під сумнів.

При проведенні аналізу балансу підприємства, насамперед здійснюють класифікацію активів підприємства за їх ліквідністю та пасивів за терміновістю оплати (табл. 2.1 та табл. 2.2).

Таблиця 2.1

Класифікація активів підприємства

Умовне позначення	Група активів, тис. грн.	30.09. 2021	31.12. 2020	31.12. 2019	31.12. 2018
А1	Високоліквідні (до 1 міс.)	194 028	301 067	111 201	624 915
А2	Швидколіквідні (1 - 3 міс.)	439 424	85 242	69 295	26 913
А3	Повільноліквідні (3 - 12 міс.)	895 982	135 777	203 595	113 986
Всього поточні (оборотні) активи	-	**1 529 434**	**522 086**	**384 091**	**765 814**
А4	Важколіквідні (понад 12 міс.)	80 018	857 222	544 074	247 999
Всього активів	-	**1 609 452**	**1 379 308**	**928 165**	**1 013 813**

Таблиця 2.2

Класифікація пасивів підприємства

Умовне позначення	Група пасивів, тис. грн.	30.09. 2021	31.12. 2020	31.12. 2019	31.12. 2018
П1	Найбільш термінові (до 1 міс.)	709 042	502 015	297 449	411 022
П2	Короткострокові (1 - 12 міс.)	374 671	61 355	86 642	28 714
Всього поточних зобов'язань	-	**1 083 713**	**563 370**	**384 091**	**439 736**
П3	Довгострокові (понад 12 міс.)	0	267 182	22 868	43 870
Всього зобов'язань		**1 083 713**	**830 552**	**406 959**	**483 606**
П4	Постійні (Власний капітал)	525 739	548 756	521 206	530 207
Всього	-	**1 609 452**	**1 379 308**	**928 165**	**1 013 813**

пасивів					

Таблиці 2.1 та 2.2 було заповнено на основі даних із Додатку А, складеного на основі квартальних і річних фінансових звітів АТ «Банк ¾». З даними звітами можна ознайомитися на сайті банку, оскільки вони надто об’ємні для включення їх до Додатків [16].

При оцінці ліквідності розраховують три основні коефіцієнти:

- коефіцієнт покриття;
- коефіцієнт швидкої ліквідності;
- коефіцієнт абсолютної ліквідності.

Ці показники розраховуються на підставі даних Додатка А, шляхом зіставлення поточних активів і поточних зобов’язань підприємства.

Коефіцієнт покриття (інші найменування цього коефіцієнта – коефіцієнт загальної ліквідності, коефіцієнт поточної ліквідності). Він дає загальну оцінку ліквідності активів, показуючи, яка сума поточних активів підприємства припадає на одну гривню поточних зобов’язань. Якщо поточні активи перевищують за величиною поточні зобов’язання, підприємство може розглядатися як таке, що успішно функціонує. Коефіцієнт розраховується за формулою (2.1):

(2.1)

Коефіцієнт швидкої ліквідності (інше найменування цього коефіцієнта – коефіцієнт “лакмусового папірця”). На відміну від попереднього, він враховує якість оборотних активів і є більш суворим показником ліквідності, оскільки при його розрахунку враховуються найбільш ліквідні поточні активи (запаси не враховуються). Швидкий коефіцієнт розраховується за формулою (2.2):

$$\frac{А1 + А2}{П1 + П2} \quad (2.2)$$

Коефіцієнт абсолютної (миттєвої) ліквідності (Платоспроможність) показує, яка частина поточних (короткострокових) зобов'язань може бути погашена негайно. Коефіцієнт розраховується за формулою (2.3):

$$\frac{А1}{П1 + П2} \quad (2.3)$$

Для оцінки платоспроможності і фінансової стійкості не тільки розраховують співвідношення між поточним активами і поточними зобов'язаннями, але також визначають і їх різницю.

Різниця між поточними активами і поточними зобов'язаннями становить чистий робочий капітал підприємства (Рк). Наявність чистого робочого капіталу свідчить про те, що підприємство здатне не тільки сплатити поточні борги, але й має в своєму розпорядженні фінансові ресурси для розширення діяльності і здійснення інвестицій. Розраховується за формулою (2.4):

(2.4)

Усі показники розглянуті вище розраховано і представлено у табл.2.3. Також в ній вказано нормативні значення кожного показника.

Таблиця 2.3

Ліквідність та платоспроможність

Показник	Формула	Нормативне значення	09.30. 2021	12.31. 2020	12.31. 2019	12.31. 2018
Коефіцієнт покриття (коефіцієнт поточної ліквідності)	(А1+А2+А3)/(П1+П2)	1 - 2 - ліквідний баланс, 1 - критичне значення, <1 - неліквідний баланс	1,4	0,9	1,0	1,7

Закінчення табл. 2.3

Показник	Формула	Нормативне значення	09.30. 2021	12.31. 2020	12.31. 2019	12.31. 2018
Коефіцієнт швидкої (критичної) ліквідності	(А1+А2)/ (П1+П2)	1 - нижнє значення, 0,6 - 0,9 - допустиме значення	0,6	0,7	0,5	1,5
Коефіцієнт абсолютної (миттєвої) ліквідності (Платоспромо жність)	А1/ (П1+П2)	не менше 0,2	0,2	0,5	0,3	1,4
Чистий робочий капітал підприємства, грн.	(А1+А2+А3)-(П1+П2)	більше 1	445 721, 00	- 41 284, 00	0,00	326 078 ,00

Основними показниками, які характеризують прибутковість банку, є такі:

- норма прибутку на капітал (рентабельність капіталу);
- рентабельність (прибутковість) активів;
- чиста процентна маржа.

Норма прибутку на капітал (Rк) характеризує ефективність використання капіталу і розраховується як відношення чистого прибутку (ЧП) до балансового капіталу (К). Даний коефіцієнт показує, скільки чистого прибутку припадає на 1 грн капіталу банку і характеризує економічну віддачу капіталу. У світовій практиці норма прибутку на капітал (ROE) є

основним показником ефективності діяльності банку. Норма прибутку на капітал розраховується за формулою (2.5):

$$R_к = \frac{ЧП}{К} \times 100\% \quad (2.5)$$

Рентабельність активів (Ra) визначається відношенням чистого прибутку до сукупних активів банку, тобто до ресурсів, що управляються. Даний показник відображає внутрішню політику банку, професіоналізм його менеджерів, які підтримують оптимальну структуру активів і пасивів з погляду доходів і витрат. Тому у світовій практиці багато спеціалістів вважають даний показник (ROA) найкращим показником для оцінювання ефективності роботи менеджерів банку. Розраховується по формулі (2.6):

$$R_а = \frac{ЧП}{А} \times 100\% \quad (2.6)$$

Чиста процентна маржа (ЧПМ) дає змогу оцінити здатність банку утворювати чистий процентний дохід, використовуючи загальні активи. До деякої міри можна вважати, що цей показник характеризує ефективність структури активів банку. Чиста процентна маржа обчислюється як відношення чистого процентного доходу (ЧПД) до загальних активів банку (А). Розраховується по формулі (2.7):

, (2.7)

де ПД – процентний дохід;

ПВ – процентні витрати.

Розраховані показники представлено у табл. 2.4.

Таблиця 2.4

Показники рентабельності банку

Показники	Формула	Оптимальне значення, %	30.09.2021 - 31.12.2020	31.12.2020 - 31.12.2019	31.12.2019 - 31.12.2018
Рентабельність капіталу (ROE), %	(Прибуток після оподаткуваня/(Власний капітал на початок періоду+Власний капітал на кінець періоду)/2)*100	оптимальне ≥ 10, критичне ≥1	3,2	4,1	3,0
Рентабельність активів (ROA), %	(Прибуток після оподаткуваня/(Активи на початок періоду+Активи на кінець періоду)/2)*100	≥ 1	1,2	1,9	1,6

Закінчення таблиці 2.4

Показники	Формула	Оптимальне значення, %	30.09.2021 - 31.12.2020	31.12.2020 - 31.12.2019	31.12.2019 - 31.12.2018
Чиста процентна маржа, %	((Процентні доходи - Процентні витрати)/(Активи на початок періоду+Активи на кінець періоду)/2)*100	4,5	6,0	9,4	9,2

Розрахунки проведено на основі даних Додатку Б та Додатку В.

Проаналізуваши результати розрахунків ліквідності та рентабельності, можна зробити висновок, що гроші на покращення інформаційної безпеки в підприємства є.

2.2 Аналіз інформаційної безпеки банку

Формування інформаційної безпеки банківських установ та забезпечення ефективного захисту інформації є надзвичайно актуальним, оскільки щоденно обробляється великий обсяг інформації різного рівня конфіденційності.

З огляду на результати проведених досліджень, вивчаючи наукові праці вітчизняних і зарубіжних авторів, а також специфіку діяльності банківських установ, під поняттям «інформаційна безпека банку» ми розуміємо стан захищеності всіх інформаційних активів банку від внутрішніх і зовнішніх загроз. При цьому під інформаційними активами ми розуміємо будь-яку

інформацію, що має цінність для банківської установи, систему її обробки або місце зберігання.

Відповідно до статті 60 Закону України “Про банки і банківську діяльність”: “Інформація щодо діяльності та фінансового стану клієнта, яка стала відомою банку у процесі обслуговування клієнта та взаємовідносин з ним або стала відомою третім особам при наданні послуг банку або виконанні функцій, визначених законом, а також визначена у цій статті інформація про банк є банківською таємницею” [1].

Керівництвом АТ “Банк ¾” затверджено “Політику інформаційної безпеки акціонерного товариства “Банк ¾”.

Політика розроблена відповідно до Положення про організацію заходів із забезпечення інформаційної безпеки в банківській системі України, затвердженого постановою Правління Національного банку України від 28.09.2017 № 95, Національних стандартів України ДСТУ ISO/IEC 27000:2015 «Методи захисту система управління інформаційною безпекою. Огляд і словник», ДСТУ ISO/IEC 27001:2015 «Методи захисту системи управління інформаційною безпекою. Вимоги», ДСТУ ISO/IEC 27002:2015 «Звід практик щодо заходів інформаційної безпеки», вимог законодавства України та нормативно-правових актів Національного банку України, а також вимог міжнародних та внутрішньодержавних платіжних систем та систем переказу коштів.

У Банку створений та постійно діє Керівний орган з питань впровадження та функціонування Системи інформаційної безпеки, який очолює Голова Правління, та до складу якого входять керівники підрозділів, що є власниками, або активними учасниками критичних бізнес-процесів. Кожен співробітник Банку забезпечує підтримку відповідного рівня інформаційної безпеки Банку. В своїй роботі всі підрозділи та працівники дотримуються вимог Політики інформаційної безпеки та несуть відповідальність за їх порушення згідно з чинним законодавством України та внутрішньобанківськими нормативними документами. Всі працівники Банку

зобов’язані негайно звітувати керівництву про інциденти інформаційної безпеки, а керівництво приймає на себе зобов’язання негайно реагувати на такі інциденти шляхом усунення наслідків та причин їх виникнення.

Відповідно до Політики інформаційної безпеки банку, її ціллю є впровадження, ефективне функціонування, регулювання та підтримка системи управління інформаційною безпекою, яка забезпечує захист інформації та ресурсів Банку від зовнішніх і внутрішніх загроз та загроз, які пов'язані з навмисними та ненавмисними діями працівників Банку, а також контрагентів Банку, третіх осіб, забезпечує безперервну роботу Банку, сприяє мінімізації ризиків операційної діяльності Банку та створює позитивну репутацію Банку при роботі з клієнтами. Цілями інформаційної безпеки Банку є збереження конфіденційності, цілісності, доступності інформації. захист інформаційних ресурсів Банку від зовнішніх та внутрішніх загроз.

Дія Політики поширюється на весь Банк в цілому. Всі працівники Банку, незалежно від рівнів доступу до інформації та ресурсів Банку, мають дотримуватись вимог цієї Політики. Вона використовується для усіх критичних бізнес-процесів/банківських продуктів/програмно-технічних комплексів Банку.

Основними принципами Політики є підтримання належного захисту інформації із забезпеченням цілісності, конфіденційності, доступності та спостережності, насамперед інформації з обмеженим доступом.

Цілісність – властивість точності та повноти інформації.

Конфіденційність – властивість інформації не ставати доступною та розкритою для несанкціонованих осіб, об'єктів або процесів.

Доступність – властивість досяжності й можливості використання на вимогу авторизованого об’єкта, яка полягає в тому, що користувач і/або процес, який володіє відповідними повноваженнями, може отримати доступ до інформації або використовувати ресурс відповідно до правил, встановлених цією Політикою, у визначений проміжок часу.

Спостережність – властивість системи, що дозволяє фіксувати діяльність користувачів і процесів, використання пасивних об’єктів, а також однозначно установлювати ідентифікатори причетних до певних подій користувачів і процесів з метою запобігання порушення цієї Політики і/або забезпечення відповідальності за певні дії.

Всі працівники Банку до того, як вони приступають до виконання своїх обов’язків, дають письмове зобов’язання щодо збереження банківської таємниці та іншої інформації з обмеженим доступом, яке залишається чинним протягом всього періоду роботи в Банку та після їх звільнення необмежений час.

При забезпеченні інформаційної безпеки Банк керується ризик-орієнтованим підходом, який забезпечує розуміння, моніторинг та зменшення ризиків діяльності. Банк обробляє ризики інформаційної безпеки відповідно до внутрішньої методології, на підставі оцінки ймовірності реалізації ризиків та важкості їх наслідків, визначає три рівні ризиків: високий, середній та низький. Банк має право прийняти ризик будь-якого рівня, проте рішення про прийняття високого рівня ризику має прийматись керівництвом на підставі повної поінформованості, аналізу загроз та за умов здійснення дієвих заходів зі зменшення рівня ризику (в тому числі впровадження компенсаційних заходів).

Банком використовуються наступні методи щодо забезпечення інформаційної безпеки:

- створено та затверджено перелік відомостей та носіїв інформації, що містить конфіденційну інформацію та банківську таємницю;
- створено та затверджено перелік критичних бізнес-процесів, за якими проводиться оцінка ризиків інформаційної безпеки та подальша їх обробка;
- встановлено правила доступу до інформаційних ресурсів та програмно-технічних комплексів;
- забезпечується контроль фізичного та логічного доступу до всіх

визначених ресурсів Системи управління інформаційною безпекою у Банку;

- забезпечується парольний захист програмних та сервісних ресурсів;
- забезпечується антивірусний захист та захист від зловмисного коду;
- забезпечується захист мережі;
- забезпечується ідентифікація та автентифікація всіх визначених ресурсів;
- забезпечується криптографічний захист інформації;
- проводяться процедури для визначення, чи мала місце якась компрометація ресурсів Системи управління інформаційною безпекою, внутрішні аудити Системи управління інформаційною безпекою та аналіз Системи управління інформаційною безпекою з боку керівництва Банку;
- проводяться процедури захисту інформації при її передачі третім особам, укладаються угоди про конфіденційність, та здійснюються заходи для забезпечення повернення чи знищення інформації та ресурсів Системи управління інформаційною безпекою по закінченні або в погоджений момент часу протягом дії угоди;
- забезпечується формування та збереження відокремлених електронних даних;
- забезпечується резервне копіювання інформації та створення резерву апаратних комплексів;
- моніторинг та вдосконалення Системи управління інформаційною безпекою.

Для дистанційного обслуговування клієнтів функціонує інформаційна система Інтернет-банкінг. Високий рівень інформаційної безпеки під час експлуатації Інтернет-банкінгу забезпечується наступними механізмами:

- Автентифікація серверу Інтернет-банкінгу - для захисту від атак, спрямованих на підміну банківського Web-сервера і модифікації його контенту (під час передачі даних застосовується протокол SSL (Secure Sockets Layer).
- Автентифікація клієнтів Інтернет-банкінгу - для безпечного доступу до

системи застосовується технологія двофакторної аутентифікації користувачів.

- Шифрування даних - для забезпечення конфіденційності даних, якими обмінюються користувачі з Банком по каналах Інтернет-банкінгу, ці дані шифруються. Таким чином, виключається можливість перехоплення та несанкціонованого читання платіжної та іншої інформації.

Інформаційні системи та внутрішні мережі Банку відповідають вимогам стандартів з інформаційної безпеки, керівництво сприяє проведенню модернізації обладнання.

У Банку розробляється, діє, тестується та оновлюється план забезпечення безперервної діяльності, у якому враховано пріоритет Банку щодо забезпечення безперервної діяльності критично важливих інформаційних систем, заходи відновлення інформаційних систем після збоїв. Приймаючи ризик-орієнтований підхід до планування діяльності, Банк ідентифікує та оцінює альтернативні варіанти оброблення ризиків та обирає конкретний захід безпеки в процесі забезпечення безперебійної діяльності, виходячи з імовірності настання загроз, швидкості та ефективності заходу з оброблення ризиків та особистого професійного досвіду фахівців Банку.

Банк вимагає від всього персоналу бути обізнаними та виконувати вимоги інформаційної безпеки в роботі, сприяє створенню належного інформаційного поля для підвищення рівня знань працівників. Вимоги щодо освітнього рівня працівників Банку встановлюються в їх посадових інструкціях, і для персоналу, задіяного у критичних бізнес-процесах, встановлюється критерій наявності вищої освіти. Працівники Банку та особи, що одержують доступ до інформаційних ресурсів Банку, обов’язково проходять вступний документований інструктаж з питань інформаційної безпеки. Банк у вступних інструктажах, пам’ятках, угодах про конфіденційність попереджає про відповідальність за порушення вимог з інформаційної безпеки, аж до кримінальної. Для зменшення ризиків виникнення інцидентів інформаційної безпеки керівництво Банку створює

умови для систематичного навчання працівників нормам та заходам інформаційної безпеки. Враховуючи розмір Банку, керівництво Банку зобов'язує керівників структурних підрозділів вести постійну роз'яснювальну роботу та здійснювати неухильний контроль за дотриманням підлеглими вимог з інформаційної безпеки.

Банк застосовує процедури захисту інформації:

- обізнаність персоналу — надання кожним окремим працівником зобов'язання щодо збереження банківської таємниці та іншої інформації з обмеженим доступом та обізнаність (усвідомлення) персоналу з відповідальністю за незаконне використання та розголошення інформації з обмеженим доступом;
- застосування дисциплінарних процесів щодо порушників інформаційної безпеки;
- апаратні, програмні засоби, в тому числі засоби сканування інформаційних систем, засоби відеоспостереження;
- розмежування та контроль доступів, ієрархія санкціонування доступів та періодичний перегляд доступів до інформаційних систем Банку;
- використання застережень про нерозголошення та захист інформації з обмеженим доступом та дотримання вимог цієї Політики у відносинах з третіми особами, що одержують доступ до інформаційних ресурсів Банку;
- ідентифікація всіх осіб, що одержують доступ до інформаційних систем Банку;
- резервне копіювання, архівування та інші заходи на розсуд Банку.

РОЗДІЛ 3 РОЗРОБКА ЗАХОДІВ ПОКРАЩЕННЯ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ БАНКУ

3.1 Розробка заходів покращення інформаційної безпеки

Банк, як і будь-яке інше підприємство кожного дня оброблює досить багато інформації на паперових носіях. Звіти, заяви, службові записки і т.і. Візування документів займає досить багато часу, а зберігання паперової документації – багато місця. Тому я пропоную впровадити електронний документообіг та електронний архів для зберігання інформації.

По-перше, таке рішення значно зекономить час на візуванні документів. Весь процес займає лічені хвилини, без необхідності покидати робоче місце. А зважаючи на ситуацію з пандемією і віддалену роботу, навіть не покидаючи власної оселі.

По-друге, це більш безпечно, менше ризик, що дані стануть відомі третім особам.

По-третє, швидший та зручніший обмін даними між підрозділами, які знаходяться поза межами головного офісу.

В підтвердження надаю дані проведеного анонімного опитування, серед 115 респондентів з різних галузей, різного віку та різного ступеню обізнаності. Як видно на рис.3.1, 56% опитуваних негативно відносяться до паперового документообігу, 28% нейтрально і тільки 16% вважають, що це зручно. Тоді як про електронний документообіг думки вже зовсім інші. 72% вважають його зручним, 20% байдуже і тільки 8% вважають, що це незручно. Враховуючи, що 24% опитуваних віком від 45 років, можна списати 16%, які підтримують паперові документи і 8%, які не підтримують електронні на вік. Більше того, на питання «Чи хотіли б ви заміни паперового документообігу на електронний на вашому підприємстві?» 68% відповіли позитивно. Тоді як

тільки 12%, негативно. 20% невпевнених скоріш за все не впевнені, що така заміна буде повною і законною.

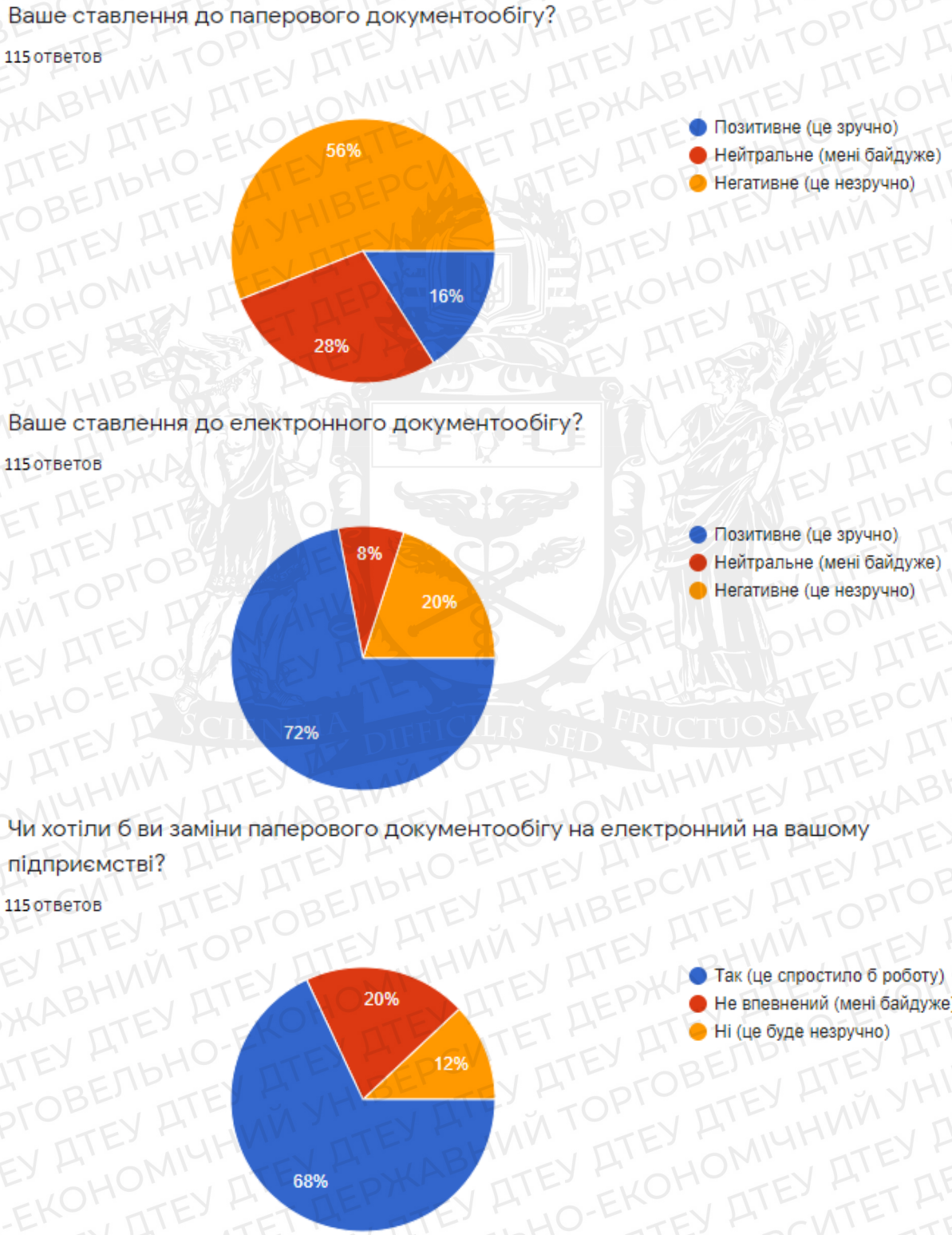

Рис. 3.1 Результати опитування

Проте, електронний документообіг та, відповідно, електронні документи в Україні є цілком легітимними, що регламентовано Законом України "Про електронні документи та електронний документообіг" від 22.05.2003 р. № 851-IV. Більше того наразу Верховною Радою розглядається закон про повний перехід на елетронний документообіг державних установ, а отже й усіх інших підприємств. Наразу це тільки питання часу.

Юридичної сили електронний документ набуває після підписання кваліфікованим електронним підписом (КЕП) — відповідно до Ст. 1 Закону №45 Закону України «Про електронні довірчі послуги»

Електронний документ, завірений кваліфікованим електронним підписом, рівноцінний паперовому і не потребує жодних копій, зроблених на інших носіях.

Кваліфікований електронний підпис має таку ж юридичну значущість, як і власноручний підпис та печатка на папері. Процес отримання і використання кваліфікованого електронног підпису регламентує Закон України «Про електронні довірчі послуги» та контролює Міністерство юстиції України.

Електронний документообіг - це життєвий цикл електронних документів в організації, починаючи від їх отримання (введення, електронна пошта і т.і.), проходження в підрозділах зі зміною стану (доведений до відома, узгоджений, підписаний, в роботі, закритий і т.і.) і закінчуючи списанням в архів. Часто електронний документообіг позначається терміном workflow , який характеризує рух документів як потік робіт, виконуваних в рамках того чи іншого бізнес-процесу. Система електронного документообігу (СЕД) - це програмне забезпечення, головними завданнями якого є організація і підтримка життєвого циклу електронних документів.

Проаналізувавши різні системи електронного документообігу, було вирішено обрати FossDoc. Це рішення на платформі FossLook, призначене для створення електронного архіву документів, організації корпоративного документообігу (workflow) і автоматизації бізнес-процесів на підприємствах,

в установах і організаціях будь-якого роду діяльності. Програма дозволяє вирішити велику кількість завдань, реалізація яких покладена на відповідні модулі. Система може бути легко перелаштована з урахуванням специфіки роботи кожного конкретного підприємства.

Загалом уявлення про програму можна скласти із рис. 3.2:

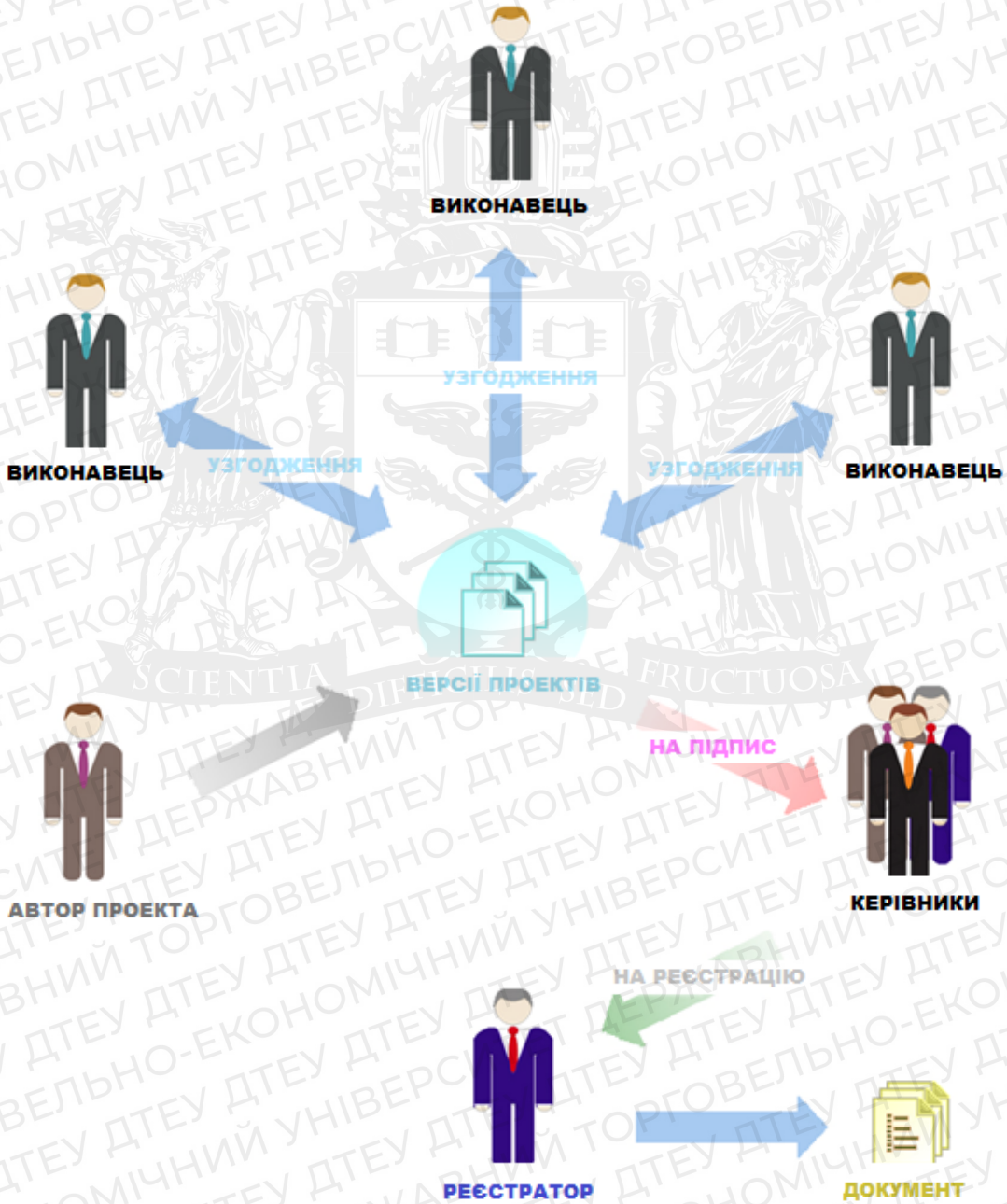

Рис. 3.2 Схематичне зображення шляху документа у системі електронного документообігу FossDoc

Як показано на рисунку, документ від автора направляється на

узгодження виконавцям, вони вносять свої правки. Далі кінцева версія відправляється керівництву на підпис і на реєстрацію. Після чого маємо готовий для роботи документ. Зазвичай увесь шлях займає не більше 10-15 хвилин.

Програмне забезпечення побудовано на основі класичної клієнт-серверної архітектури, до складу якої входять:

- Сервер FossDoc — сервер додатків, який реалізує бізнес-логіку і здійснює взаємодію клієнтських програм з сервером системи управління базами даних. Модулі, що визначають функції системи, підключаються до сервера додатків. Таким чином, продукти розрізняються серверними частинами, які містять різні набори модулів.
- Web-сервер — дозволяє працювати з сервером додатків за допомогою звичайного веб-браузера. Реалізований у вигляді зовнішнього модуля, що підключається до сервера додатків.
- База даних — управляється за допомогою сервера системи управління базами даних (My SQL, Microsoft SQL Server або Oracle). Зберігає документи, довідники, інформацію про користувачів, налаштуваннях і т.д.
- FossDoc Client — клієнтський windows-додаток, автоматизоване робоче місце (АРМ) користувача. За допомогою цієї програми звичайний користувач підключається до сервера додатків (по локальній мережі або інтернету) і вирішує свої службові завдання, як співробітник підприємства (організації). Одночасно автоматизоване робоче місце користувача є поштовим клієнтом і може приймати-відправляти листи за допомогою зовнішніх поштових серверів.
- FossDoc Web Client — веб-інтерфейс (Веб-кліент), який реалізує ті ж функції робочого місця користувача, що і windows-програма FossDoc Client, за допомогою звичайного веб браузера. Роботу веб-клієнта забезпечує веб-сервер системи.

- FossDoc Адміністратор — клієнтська програма, майстер адміністрування (автоматизоване робоче місце адміністратора). За допомогою даного програмного забезпечення проводиться адміністрування сервера додатків (введення користувачів, розподіл прав доступу, підключення додаткових функцій, проектування маршрутів, створення нових типів документів і т.д.).

Розглянемо основні функції програми:

- Автоматизація діловодства - система автоматизує всі аспекти сучасного діловодства: створення реєстраційно-контрольних карток, РКК (карток документа); відправку доручень (аналог "бігунка" в звичайному документообігу); облік паперових оригіналів за допомогою спеціальних журналів; здійснення контролю над виконанням документів; підготовку резолюцій; роботу з електронно-цифровим підписом, генерацію звітів.
- Підтримка різних типів документів - все різноманіття документів, з якими працюють користувачі, розділяється на окремі категорії - типи документів. В системі існують зумовлені типи документів (поширені у вітчизняному діловодстві): вхідні та вихідні листи, звернення громадян, службові записки, накази і т.д. Документи можуть посилатися на інші документи або бути дочірніми по відношенню до головних. Поля документів можуть заповнюватися значеннями з довідників.
- Проектування документів (бібліотеки) - є можливість налаштувати під себе продукт за допомогою функціональності бібліотек документів: додати або видалити поля і/або функції документів, налаштувати довідники. Можна спроектувати власні типи документів, а також шаблони друкарських форм, які будуть відповідати тільки заданому діловодства. Система дозволяє створювати нові документи на базі існуючих, використовуючи механізм успадкування.

- Гнучка маршрутизація документів – система електронного документообігу дозволяє гнучко налаштувати маршрути руху документів між підрозділами підприємства, вказати їх порядок виконання, узгодження, підпису, реєстрації і т.д. Є можливість налаштувати реєстрацію в декількох канцеляріях організації. Підтримується ефективний механізм створення документа на основі його проекту з фіксацією кожної стадії узгодження в окремій версії проекту.
- Підтримка колективної роботи користувачів - за допомогою довідника підрозділів можна спроектувати віртуальну структуру підприємства (організації) будь-якої складності. Рольова модель поведінки користувачів дозволить співробітникам швидко освоїти функції системи і ефективно замінювати одного користувача іншим (виконання обов'язків). Надаються потужні засоби розподілу доступу до загальних ресурсів підприємства і колективної роботи над документами.
- Вбудований поштовий сервер - поштовий сервер призначений для створення "внутрішніх" поштових скриньок користувачів (на внутрішньому домені) і роботи з ними - прийому/відправки повідомлень. Сервер також ініціює прийом повідомлень з інших поштових серверів (ukr.net, gmail.com і т.п.), а також відправку ними повідомлень, якщо у користувачів, зареєстрованих на сервері, є зовнішні поштові скриньки.
- Електронний цифровий підпис - в системі підтримується робота з електронним цифровим підписом (ЕЦП). Це дозволяє підписувати документи і їх поля за допомогою електронного цифрового підпису. Такий підпис гарантуватиме цілісність і автентичність відбитку даного документа. Ніхто, крім автора документа, не зможе внести зміни в нього так, щоб про це не стало відомо під час перевірки електронним цифровим підписом.

Інсталяція системи електронного документообігу FossDoc і введення її в експлуатацію проводиться в кілька етапів:

- Перший етап — визначення типів документів, що циркулюють в організації Замовника, і полів, що їх описують. Перелік основних типів документів надається в типовому рішенні і може бути розширений за бажанням Замовника. На цьому ж етапі визначаються основні бізнес-процеси і типові маршрути руху документів.
- Другий этап — проектування віртуальної структури організації. На даному етапі необхідно задати загальну структуру організації у вигляді деревовидного списку.
- Третій етап — визначення базових ролей співробітників у кожному підрозділі. Роль визначає можливості співробітника в системі, однак не є жорстко заданою і може бути доповнена новими правами (опції).
- Четвертий етап — підготовка базової системи для впровадження в дослідну експлуатацію, імпорт користувачів із Active Directory, призначення ролей, прав доступу, підготовка відсутніх типів документів і типових маршрутів руху документів. Навчання технічних фахівців і користувачів системи. Дослідна експлуатація системи.
- П'ятий етап — доробка системи за результатами дослідної експлуатації. Введення системи в промислову експлуатацію.

За попередніми розрахунками вартіть програми разом із встановленням та супроводженням 16 392$ (464 219грн). Послуги, які входять до програми за ці кошти:

- Платформа FossLook;
- Сховище;
- Резолюції;
- Проекти документів;
- Періодичні задачі;
- Службові записки;
- Журнал;

- Історія;
- Web-сервер;
- Доменна авторизація;
- Контроль документів;
- Аудит;
- Статистика;
- Повідомлення маршрутизації;
- Архівний сервер;
- Електронний цифровий підпис;
- Провайдер Баз Даних;
- Послуги по встановленню програмного забезпечення;
- Послуги по навчанню персоналу.

Також, в якості доповнення, необхідно провести семінар з навчання персоналу роботі з програмою та інформаційної безпеки.

Приблизний план семінару може виглядати так:

- Лекція про загальні відомості з інформаційної безпеки (що це, яку відіграє роль у розвитку підприємства, основні загрози і т.д.).
- Лекція про інформаційну безпеку банку.
- Тестові та практичне завдання на розуміння пройденого матеріалу.
- Розгляд конкретних кейсів з покращення інформаційної безпеки кожним підрозділом (сформовано на основі вимог підприємства і актуальних загроз інформаційної безпеки).
- За бажанням індивідуальні завдання для кожного підрозділу про пройденим темам.

В середньому подібний семінар буде коштувати 7000$ (198 291грн). Краще проводити в офлайн форматі і розбивати матеріал на 2-3 дні. Також не зайвим буде проведення атестації співробітників кожні півроку і оновлення їхніх знань, відповідно до змін в інформаційній безпеці.

3.2 Оцінка ефективності запропонованих рішень

Для оцінки ефективності запропонованих рішень, було розраховано низку показників, за результатами яких зроблено висновки. Результати представлено в табл. 3.1:

Таблиця 3.1

Оцінка ефективності заходів покращення ІБ банку

Показник	Умовне позначення	Формула	Оптимальне значення	Фактичне значення
Початкові інвестиції (витрати), грн.	IC	-	-	662 510
Дисконтна процентна ставка, % (прогнозний рівень інфляції)	r	-	-	8%

Закінчення таблиці 3.1

Показник	Умовне позначення	Формула	Оптимальне значення	Фактичне значення
Прогнозний грошовий потік в результаті заходів покращення, грн.	CF	-	-	-
перший рік	CF1	-	-	260 000
другий рік	CF2	-	-	275 000
третій рік	CF3	-	-	305 000
Середній прогнозний грошовий потік за рік, грн.	CFc	(CF1+CF2+ +CF3)/3	-	280 000
Період окупності, рік	PP	IC/CFc	< 3,5	2,37
Коефіцієнт рентабельності заходів покращеня, %	ARR, ROI	(CFc/IC)*100	> 0	42
Чиста приведена вартість, грн. (за три роки)	NPV	$\sum_{i=1}^{n} \frac{CF_i}{(1+r)^i} - -IC$ n, i - кількість періодів (років)	> 0	56 118

Індекс прибутковості проекту, %	PI	(NPV/IC)*100	> 1	8

Розглянемо приведені дані більш детально.

Початкові інвестиції (IC) - це сума вартості запропонованих рішень.

Прогнозний рівень інфляції (r) – це значення інфляції у %, в даному випадку, на 2022рік.

Прогнозний грошовий потік в результаті заходів покращення (CF) – це кошти, які організація планує заробити за рахунок модернізації.

Середній прогнозний грошовий потік за рік (CFc) – середнє арифметичне від CF.

Період окупності (PP) – це відрізок часу, за який організація поверне кошти, вкладені в модернізацію.

Коефіцієнт рентабельності заходів покращеня (ARR, ROI) - показник відображає прибутковість об'єкта інвестицій без урахування дисконтування.

Чиста приведена вартість (NPV) - показник, що відображає зміну грошових потоків і показує різницю між дисконтованими грошовими доходами і витратами.

Індекс прибутковості проекту (PI) - показник ефективності проекту, який показує віддачу (прибутковість) вкладеного капіталу. Індекс прибутковості являє собою відношення поточної вартості майбутніх грошових потоків до вартості початкових інвестицій. Економічний зміст даного коефіцієнта – це оцінка додаткової цінності на кожну вкладену гривню. Якщо вкладення в проект здійснюються не одноразово, а протягом усього часу реалізації, то необхідно інвестиційний капітал (*IC*) привести до єдиної вартості, тобто дисконтувати його.

Аналізуючи розрахунки, можна зробити висновки, що період окупності даних покращень приблизно 2 роки і 5 місяців. Це означає, що їх впровадження є доцільним. Більше того, індекс прибутковості проекту складає 8 балів, що є достатньо оптимістичним прогнозом.

Якщо ж говорити про загальні покращення, то можна виділити:

- Скорочення часу на формування, обробку, узгодження і візування документів.
- Підвищення загального рівня обізнаності співробітників, що в свою чергу підвищує рівень захищеності підприємства.
- Зменшення кількості паперової документації, а отже звільнення місця під інші потреби підприємства.

ВИСНОВКИ

Під час написання випускної кваліфікаційної роботи було сформульовано сутність поняття інформаційна безпека. Розглянуто головні аспекти її формування. Докладно розібрано усі загрози та шляхи їх походження. Розглянувши всі аспекти інформаційної безпеки і дослідивши її загрози, не зайвим буде ще раз звернути увагу на її значущість. Також докладно досліджено інформаційну безпеку банківської установи на прикладі АТ «Банк ¾», визначено сутність понять банківська таємниця та інформація з обмеженим доступом.

Захист інформації забезпечує необхідний рівень впевненості при розвитку підприємства. А якщо розглядати саме банк, то було практично доведено, що організація ефективної системи захисту інформації стає критично важливим стратегічним чинником розвитку та напряму впливає на темпи зростання, позицію на ринку та рівень довіри клієнтів та партнерів до організації.

Було зроблено висновки після проведеного опитування з приводу актуальності систем документообігу, які наразі впроваджено на підприємствах різних галузей. 56% респондентів незадоволені паперовим документообігом і 68% з радістю б перейшли на електронний. Ці результати вкотре підтверджують актуальність теми та обраних заходів покращення.

Також доцільним буде згадати про розрахунок показників ефективності, рентабельності та ліквідності підприємства за останні три роки, зроблених на основі фінансової звітності АТ «Банк ¾». Було виявлено, що незважаючи на пандемію та складну економічну ситуацію, підприємство підвищує доходи та знижує витрати.

Під час виконання випускної кваліфікаційної роботи було вирішено такі завдання:

- досліджено концептуальні засади інформаційної безпеки;

- проаналізовано фінансово-економічну діяльність підприємства;
- проаналізувано інформаційну безпеку підприємства;
- розроблено заходи для покращення інформаційної безпеки на підприємстві;
- оцінено ефективність запропонованих рішень.

Таким чином, завдання вирішені в повному обсязі, мета досягнута - розроблено управлінські рішення, щодо покращення інформаційної безпеки підприємства.

На підставі зробленого дослідження, можна зробити висновок, що запропоновані рішення є актуальними і допоможуть у розвитку і підвищенні доходів банку. Прогнозований дохід в результаті впровадження запропонованих заходів в середньому за три роки становить 280 000грн, а чиста приведена вартість 56 118грн. Більше того, індекс прибутковості проекту складає 8 балів, що є достатньо оптимістичним прогнозом. Також вони досить швидко окупаються, всього за 2 роки і 5 місяців, навіть за умов пандемії.

На завершення можна зробити висновок, що данні дослідження і рішення можна сміливо застосовувати при покращенні інформаційної безпеки банку, оскільки невисока вартість готово програмного забезпечення з електронного документообігу, простота його встановлення та використання та підвищення обізнаності співробітників з інформаційної безпеки значно підвищать рівень захищеності та прибутки підприємства.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Про банки і банківську діяльність: Закон України від 07 грудня 2000 р. № 2121-III / Президент України URL: https://zakon.rada.gov.ua/laws /show/2121-14#Text
2. Методичні рекомендації з аналізу і оцінки фінансового стану підприємств // Верховна рада України. Законодавство України. URL: https://zakon.rada .gov.ua/rada/show/v0006626-06#top
3. Аналіз показників ліквідності і платоспроможності підприємства // Букліб. URL: https://buklib.net/books/28009/
4. Бандурка О.М., Ковальов Є. В., Садиков М. А., Маковоз О. С. Економіка підприємства: навч. посібник / за ред. О.М. Бандурки. Харків: ХНУВС, 2017, 192с.
5. Вінниченко О.В., Гудзь А.В. Фінансовий стан банку та методи його оцінки в Україні. *Вісник економіки транспорту і промисловості №6 /* Вінниченко О.В., Гудзь А.В., 2020.
6. Електронний документообіг // FossDoc. URL: https://fossdoc.com /elektronniy-dokumentooborot
7. Зубок М.І. Інформаційна безпека в підприємницькій діяльності: підручник. К: ГНОЗИС, 2015
8. Інформаційна безпека // Вікіпедія. URL: https://uk.wikipedia.org/wiki/% D0%86%D0%BD%D1%84%D0%BE%D1%80%D0%BC%D0%B0%D1%86 %D1%96%D0%B9%D0%BD%D0%B0_%D0%B1%D0%B5%D0%B7%D0% BF%D0%B5%D0%BA%D0%B0
9. Курс, інфляція, ВВП у 2022-2024 роках: консенсус-прогноз мінекономіки // FINBALANCE. URL: https://finbalance.com.ua/news/kurs-inflyatsiya-vvp-derzhborh-v-2022-2024-rokakh-konsensus-prohnoz-minekonomiki
10. Непочатенко О.О., Мельничук Н.Ю. Фінанси підприємств: підручник. К: Центр навчальної літератури, 2019, 504с.
11. Організація електронного документообігу на підприємстві // UTEKA.UA. URL: https://uteka.ua/ua/publication/commerce-12-dokumentooborot-2-organizaciya-elektronnogo-dokumentooborota-na-predpriyatii
12. Основи фінансового аналізу за даними спрощеної звітності // Облік і фінанси АПК: освітній портал. URL: http://magazine.faaf.org.ua/osnovi-finansovogo-analizu-za-danimi-sproschenoizvitnosti.html#:~:text=%D0% A1%D0%B5%D1%80%D0%B5%D0%B4%20%D0%BF%D0%B5%D1%80% D1%88%D0%B8%D1%85%20%D0%B2%D0%B8%D0%BA%D0%BE%D1

%80%D0%B8%D1%81%D1%82%D0%BE%D0%B2%D1%83%D1%8E%D1%82%D1%8C%D1%81%D1%8F%3A%20%D0%B2%D0%B0%D0%BB%D1%8E%D1%82%D0%B0%20%D0%B1%D0%B0%D0%BB%D0%B0%D0%BD%D1%81%D1%83,%D0%BB%D1%96%D0%BA%D0%B2%D1%96%D0%B4%D0%BD%D0%BE%D1%81%D1%82%D1%96%2C%20%D0%B7%D0%B0%D0%B1%D0%BE%D1%80%D0%B3%D0%BE%D0%B2%D0%B0%D0%BD%D0%BE%D1%81%D1%82%D1%96%2C%20%D0%B5%D1%84%D0%B5%D0%BA%D1%82%D0%B8%D0%B2%D0%BD%D0%BE%D1%81%D1%82%D1%96%20%D0%BF%D1%80%D0%B0%D1%86%D1%96

13. Оцінка ефективності діяльності // Букліб. URL: https://buklib.net/books/28334/
14. Оцінка ефективності інвестицій в Excel // SGV.IN.UA. URL: https://sgv.in.ua/off-lifaq/28-otsinka-efektivnosti-investitsij-v-excel-rozrakhunok-npv-pp-dpp-irr-arr-pi
15. Підвищення обізнаності персоналу, щодо інформаційної безпеки // EY. URL: https://www.ey.com/uk_ua/consulting/information-security-learning-consulting
16. ПОЛІТИКА ІНФОРМАЦІЙНОЇ БЕЗПЕКИ АКЦІОНЕРНОГО ТОВАРИСТВА «БАНК 3/4» // Банк ¾. URL: https://bank34.ua/bezpeka-obslugovuvannya/politika-informacijnoi-bezpeki.html
17. Рентабельність // Національний банк України. URL: https://old.bank.gov.ua/control/uk/publish/article?art_id=123599#:~:text=%D0%A0%D0%95%D0%9D%D0%A2%D0%90%D0%91%D0%95%D0%9B%D0%AC%D0%9D%D0%86%D0%A1%D0%A2%D0%AC%20(rate%20of%20return)%20%E2%80%93,%D0%B0%D0%B1%D0%BE%20%D0%BF%D0%BE%D1%82%D0%BE%D0%BA%D1%96%D0%B2%2C%20%D1%89%D0%BE%20%D1%97%D1%97%20%D1%84%D0%BE%D1%80%D0%BC%D1%83%D1%8E%D1%82%D1%8C.&text=%D0%B1%D0%B0%D0%BD%D0%BA%D1%96%D0%B2%D1%81%D1%8C%D0%BA%D0%BE%D1%97%20%D0%B4%D1%96%D1%8F%D0%BB%D1%8C%D0%BD%D0%BE%D1%81%D1%82%D1%96%2C%20%D1%94%20ROA%2C%20ROE
18. Фінансова звітність // Банк ¾. URL: https://bank34.ua/pro-bank/finansova-zvitnist/
19. Document Library [Електронний ресурс]. – Режим доступу : https://www.pcisecuritystandards.org/document_library?category=pcidss&document=pci_dss

Додаток А

Таблиця А.1

Аналіз активів та зобов'язань за строками їх погашення 2021 рік

	9 міс. 2021 рік, тис. грн.				
	до 1 міс.	1 - 3 міс.	3 - 12 міс.	понад 12 міс.	**Усього**
	1	2	3	4	**5**
Активи					
Грошові кошти та їх еквіваленти	188 049	0	0	0	**188 049**
Кредити та заборгованість банків	5 979	0	0	0	**5 979**
Кредити та заборгованість клієнтів	0	46 612	93 224	0	**139 836**
Інвестиції в цінні папери	0	392 812	785 625	0	**1 178 437**
Похідні фінансові активи	0	0	0	0	**0**
Інвестиційна нерухомість	0	0	0	1 357	**1 357**
Дебіторська заборгованість щодо поточного податку на прибуток	0	0	0	0	**0**
Основні засоби та нематеріальні активи	0	0	0	78 661	**78 661**
Інші активи	0	0	17 133	0	**17 133**
Всього активів	**194 028**	**439 424**	**895 982**	**80 018**	**1 609 452**
Зобов'язання					
Кошти банків	709 042	0	0	0	**709 042**
Кошти клієнтів	0	0	358 877	0	**358 877**
Похідні фінансові зобов'язання	0	0	402	0	**402**
Зобов'язання щодо поточного податку на прибуток	0	0	1 582	0	**1 582**
Відстрочені податкові зобов'язання	0	0	4 837	0	**4 837**
Інші зобов'язання	0	0	8 973	0	**8 973**
Всього зобов'язань	**709 042**	**0**	**374 671**	**0**	**1 083 713**

Продовження додатку А

Таблиця А.2

Аналіз активів та зобов'язань за строками їх погашення 2020 рік

	2020 рік, тис. грн.				
	до 1 міс.	1 - 3 міс.	3 - 12 міс.	понад 12 міс.	**Усього**
	1	2	3	4	**5**
Активи					
Грошові кошти та їх еквіваленти	148 325	0	0	0	**148 325**
Кредити та заборгованість банків	6 298	0	0	0	**6 298**
Кредити та заборгованість клієнтів	3 258	34 322	102 127	40 123	**179 830**
Інвестиції в цінні папери	114 148	50 920	33 650	749 053	**947 771**
Похідні фінансові активи	0	0	0	0	**0**
Інвестиційна нерухомість	0	0	0	1 357	**1 357**
Дебіторська заборгованість щодо поточного податку на прибуток	0	0	0	0	**0**
Основні засоби та нематеріальні активи	0	0	0	66 689	**66 689**
Інші активи	29 038	0	0	0	**29 038**
Всього активів	**301 067**	**85 242**	**135 777**	**857 222**	**1 379 308**
Зобов'язання					
Кошти банків	271 035	0	0	257 000	**528 035**
Кошти клієнтів	230 701	21 037	18 997	8 472	**279 207**
Похідні фінансові зобов'язання	279	0	0	0	**279**
Зобов'язання щодо поточного податку на прибуток	0	0	1 851	0	**1 851**
Відстрочені податкові зобов'язання	0	0	9 468	0	**9 468**
Інші зобов'язання	0	0	10 002	1 710	**11 712**
Всього зобов'язань	**502 015**	**21 037**	**40 318**	**267 182**	**830 552**

Продовження додатку А

Таблиця А.3

Аналіз активів та зобов'язань за строками їх погашення 2019 рік

	2019 рік, тис. грн.				
	до 1 міс.	1 - 3 міс.	3 - 12 міс.	понад 12 міс.	**Усього**
	1	2	3	4	**5**
Активи					
Грошові кошти та їх еквіваленти	71 098	0	0	0	**71 098**
Кредити та заборгованість банків	1 802	0	0	0	**1 802**
Кредити та заборгованість клієнтів	428	56 588	79 740	155 265	**292 021**
Інвестиції в цінні папери	12 152	12 707	123 855	298 929	**447 643**
Похідні фінансові активи	1 908	0	0	0	**1 908**
Інвестиційна нерухомість	0	0	0	1 446	**1 446**
Дебіторська заборгованість щодо поточного податку на прибуток	0	0	0	0	**0**
Основні засоби та нематеріальні активи	0	0	0	87 713	**87 713**
Інші активи	23 813	0	0	721	**24 534**
Всього активів	**111 201**	**69 295**	**203 595**	**544 074**	**928 165**
Зобов'язання					
Кошти банків	180 370	0	0	0	**180 370**
Кошти клієнтів	114 080	60 117	15 837	580	**190 614**
Похідні фінансові зобов'язання	2 999	0	0	0	**2 999**
Зобов'язання щодо поточного податку на прибуток	0	0	396	0	**396**
Відстрочені податкові зобов'язання	0	0	2 795	0	**2 795**
Інші зобов'язання	0	0	7 497	22 288	**29 785**
Всього зобов'язань	**297 449**	**60 117**	**26 525**	**22 868**	**406 959**

Продовження додатку А

Таблиця А.4

Аналіз активів та зобов'язань за строками їх погашення 2018 рік

	2018 рік, тис. грн.				
	до 1 міс.	1 - 3 міс.	3 - 12 міс.	понад 12 міс.	**Усього**
	1	2	3	4	**5**
Активи					
Грошові кошти та їх еквіваленти	304 984	0	0	0	**304 984**
Кредити та заборгованість банків	1 068	0	0	0	**1 068**
Кредити та заборгованість клієнтів	2 251	23 489	82 198	177 276	**285 214**
Інвестиції в цінні папери	316 262	3 424	3 197	0	**322 883**
Похідні фінансові активи	350	0	0	0	**350**
Інвестиційна нерухомість	0	0	0	1 447	**1 447**
Дебіторська заборгованість щодо поточного податку на прибуток	0	0	291	0	**291**
Основні засоби та нематеріальні активи	0	0	0	69 276	**69 276**
Інші активи	0	0	28 300	0	**28 300**
Всього активів	**624 915**	**26 913**	**113 986**	**247 999**	**1 013 813**
Зобов'язання					
Кошти банків	110 250	0	0	0	**110 250**
Кошти клієнтів	299 849	0	15 954	43 870	**359 673**
Похідні фінансові зобов'язання	923	0	0	0	**923**
Зобов'язання щодо поточного податку на прибуток	0	0	0	0	**0**
Відстрочені податкові зобов'язання	0	0	406	0	**406**
Інші зобов'язання	0	0	12 354	0	**12 354**
Всього зобов'язань	**411 022**	**0**	**28 714**	**43 870**	**483 606**

Додаток Б

Таблиця Б.1

Звіт про прибутки і збитки та інший сукупний дохід (Звіт про фінансові результати)

Найменування статті	**30.09.2021, тис. грн.**	**30.09.2020, тис. грн.**	**31.12.2020, тис. грн.**	**31.12.2019, тис. грн.**	**31.12.2018, тис. грн.**
Процентні доходи	121 160	105 103	143 114	133 692	112 062
Процентні витрати	(30 890)	(26 310)	(34 135)	(44 462)	(32 262)
Чистий процентний дохід	**90 270**	**78 793**	**108 979**	**89 230**	**79 800**
Комісійні доходи	34 969	32 628	46 149	40 523	46 454
Комісійні витрати	(10 220)	(11 224)	(15 437)	(11 012)	(13 499)
Чистий прибуток від операцій з активами	89 453	213 370	254 898	209 547	257 342
Чистий збиток від операцій з активами	(23 843)	(13 461)	(10 954)	(445)	(39 325)
Інші операційні доходи	570	537	739	1 099	750
Адміністративні витрати	(159 888)	(282 468)	(359 160)	(306 584)	(281 912)
Прибуток до оподаткування	**21 311**	**18 175**	**25 214**	**22 358**	**49 610**
Витрати на податок на прибуток	(3 943)	(2 191)	(3 507)	(6 739)	(2 862)
Прибуток після оподаткування	***17 368***	***15 984***	***21 707***	***15 619***	***46 748***
Інший сукупний дохід після оподаткування	**(19 763)**	**30 096**	**20 679**	**19760**	**(9 105)**
Усього сукупного	**(2 395)**	**46 080**	**42 386**	**35 379**	**37 643**

доходу					

Додаток В

Таблиця В.1

Аналіз динаміки доходів та витрат (абсолютні та відносні показники)

Період	**30.09.2021 - 30.09.2020**		**ОД***	**31.12.2020 - 31.12.2019**		**ОД***	**31.12.2019 - 31.12.2018**		**ОД***
Найменування статті	**Абсолютне зростання, тис. грн. ***	**Коефіцієнт зростання, % ****		**Абсолютне зростання, тис. грн. ***	**Коефіцієнт зростання, % ****		**Абсолютне зростання, тис. грн. ***	**Коефіцієнт зростання, % ****	
Процентні доходи	16 057	15	1	9 422	7	1	21 630	19	1
Процентні витрати	4 580	17	0	-10 327	-23	1	12 200	38	0
Чистий процентний дохід	11 477	15	1	19 749	22	1	9 430	12	1
Комісійні доходи	2 341	7	1	5 626	14	1	-5 931	-13	0
Комісійні витрати	-1 004	-9	1	4 425	40	0	-2 487	-18	1
Чистий прибуток від операцій з активами	-123 917	-58	0	45 351	22	1	-47 795	-19	0
Чистий збиток від операцій з активами	10 382	77	0	10 509	2 362	0	-38 880	-99	1
Інші операційні доходи	33	6	1	-360	-33	0	349	47	1
Адміністративні витрати	-122 580	-43	1	52 576	17	0	24 672	9	0
Прибуток до оподаткування	3 136	17	1	2 856	13	1	-27 252	-55	0
Витрати на податок на прибуток	1 752	80	0	-3 232	-48	1	3 877	135	0
Прибуток за звітний	1 384	9	1	6 088	39	1	-31 129	-67	0

період									

Період	**30.09.2021 - 30.09.2020**		**ОД*****	**31.12.2020 - 31.12.2019**		**ОД*****	**31.12.2019 - 31.12.2018**		**ОД*****
Найменування статті	**Абсолютне зростання, тис. грн. ***	**Коефіцієнт зростання, % ****		**Абсолютне зростання, тис. грн. ***	**Коефіцієнт зростання, % ****		**Абсолютне зростання, тис. грн. ***	**Коефіцієнт зростання, % ****	
Інший сукупний дохід після оподаткування	-10 333	-34	0	919	5	1	10 655	117	1
Усього сукупного доходу за звітний період	-43 685	-95	0	7 007	20	1	-2 264	-6	0
Сума оцінок динаміки			**8**			**10**			**6**

* Абсолютне зростання = значення показника на кінець періоду - значення показника на початок періоду

** Коефіцієнт зростання = ((значення показника на кінець періоду - значення показника на початок періоду) / значення показника на початок періоду)) * 100

*** Оцінка динаміки доходів та витрат (ОД): позитивна - 1, негативна - 0